Background

Pre-requisites

Risks

Warning. If you do this against multiple domain controllers you might lockout the domain user Administrator, which might not be desirable. So make sure you exclude the majority of domain-controllers.

How to check for

```
crackmapexec smb  192.1.1.0/24 -u Administrator -p password --local-auth
```

If you says "Pwn!ed" after you have successfully authenticated as the local admin.

How to exploit

Recommendation

Related Vulnerabilities

References